Wartości $\left\{ n \atop k \right\}$ dla małych n i k:

$n \backslash k$	0	1	2	3	4	5	6	7	8	9
0	1	0	0	0	0	0	0	0	0	0
1	0	1	0	0	0	0	0	0	0	0
2	0	1	1	0	0	0	0	0	0	0
3	0	1	3	1	0	0	0	0	0	0
4	0	1	7	6	1	0	0	0	0	0
5	0	1	15	25	10	1	0	0	0	0
6	0	1	31	90	65	15	1	0	0	0
7	0	1	63	301	350	140	21	1	0	0
8	0	1	127	966	1701	1050	266	28	1	0
9	0	1	255	3025	7770	6951	2646	462	36	1

Uwaga!

W przypadku, gdy $n \geqslant 0$ i $k < 0$ zakładamy, że $\left\{ n \atop k \right\} = 0$.

Twierdzenie

Wzór

$$x^{\overline{n}} = \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix} x^k$$

zachodzi dla każdej liczby całkowitej dodatniej n.

- Zauważmy, że jak w powyższym wzorze podstawimy $x = 1$, to otrzymamy jeden z omawianych wcześniej wzorów.
- Dowód powyższego twierdzenia można przeprowadzić indukcyjnie — podobnie do przeprowadzonego wcześniej dowodu analogicznego twierdzenia dla liczb Stirlinga drugiego rodzaju (należy pamiętać, że $x^{\overline{n}} = (x+n-1)x^{\overline{n-1}}$).

Potęgi kroczące

Definicja

Niech $m \geqslant 0$ będzie liczbą całkowitą.

- *Dolną silnią* nazywamy wyrażenie
$$x^{\underline{m}} = x(x-1)(x-2)\cdots(x-m+1).$$
- *Górną silnią* nazywamy wyrażenie
$$x^{\overline{m}} = x(x+1)(x+2)\cdots(x+m-1).$$

Wyrażenie $x^{\underline{m}}$ czytamy „x do m-tej ubywającej”, a $x^{\overline{m}}$ — „x do m-tej przybywającej”.

Wartości $\left\{ n \atop k \right\}$ dla małych wartości k:

- $k = 0$.
  Przyjmujemy, że $\left\{ 0 \atop 0 \right\} = 1$. Jeżeli $n > 0$ to, oczywiście, $\left\{ n \atop 0 \right\} = 0$.
- $k = 1$.
  Mamy $\left\{ 0 \atop 1 \right\} = 0$. Dla $n > 0$ istnieje dokładnie jeden n-elementowy podział n-elementowego zbioru, więc
  $$\left\{ n \atop 1 \right\} = 1.$$
- $k = 2$.
  Oczywiście $\left\{ 0 \atop 2 \right\} = 0$. Załóżmy, że $n > 0$. Chcemy rozbić zbiór $S = \{a_1, a_2, \ldots, a_n\}$ na dwa podzbiory S_1 i S_2. Bez straty ogólności możemy przyjąć, że $a_1 \in S_1$. Pozostałe a_i możemy przypisać do zbioru S_1 na 2^{n-1} sposobów, ale musimy pamiętać, że nie możemy do niego przypisać wszystkich elementów zbioru S. Zatem
  $$\left\{ n \atop 2 \right\} = 2^{n-1} - 1.$$

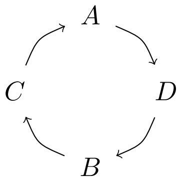
Liczby Stirlinga pierwszego rodzaju

Definicja

Cyklem nazywamy cykliczne ustawienia elementów danego zbioru.

Przykładowo jednym z cykli zbioru $\{A, B, C, D\}$ jest cykl w którym A przechodzi na D, D na B, B na C, a C na A. Ten cykl zapisujemy w postaci $[A, D, B, C]$. Oczywiście

$$[A, D, B, C] = [D, B, C, A] = [B, C, A, D] = [C, A, D, B].$$



Definicja (liczby Stirlinga pierwszego rodzaju)

Symbol $\left[n \atop k \right]$ (czyt. k cykli n) oznacza liczbę sposobów na rozmieszczenie n elementów w k rozłącznych cyklach.

Liczby szczególne

dr inż. Bartłomiej Pawlik

19 czerwca 2024

Zależności między liczbami Strilinga pierwszego i drugiego rodzaju

Zauważmy, że liczba cykli musi być co najmniej równa liczbie podzbiorów, więc mamy

$$\left\{ {n \atop k} \right\} \leqslant \left[{n \atop k} \right]$$

dla całkowitych nieujemnych n i k.

Zachodzą tzw. *wzory inwersji*:

Jeżeli $m \neq n$, to

$$\sum_{k=m}^{n} \left[{n \atop k} \right] \left\{ {k \atop m} \right\} (-1)^{n-k} = \sum_{k=m}^{n} \left\{ {n \atop k} \right\} \left[{k \atop m} \right] (-1)^{n-k} = 0$$

Przykład

Wyznacz wartość $\left[{4 \atop 2}\right]$.

Wyznaczymy liczbę podziału elementów czterolementowego zbioru $\{a, b, c, d\}$ na dwa niepuste cykle:

$$\begin{array}{llll} [a]\,[b,c,d], & [b]\,[a,c,d], & [c]\,[a,b,d], & [d]\,[a,b,c], \\ [a]\,[b,d,c], & [b]\,[a,d,c], & [c]\,[a,d,b], & [d]\,[a,c,b], \\ [a,b]\,[c,d], & [a,c]\,[b,d], & [a,d]\,[b,c]. & \end{array}$$

Zatem $\left[{4 \atop 2}\right] = 11$.

Zauważmy, że $\begin{bmatrix} n \\ k \end{bmatrix}$ oznacza liczbę permutacji n obiektów, które zawierają dokładnie k cykli. Zatem aby otrzymać liczbę wszystkich permutacji n obiektów, można zsumować wartości wyrażenia $\begin{bmatrix} n \\ k \end{bmatrix}$ dla wszystkich k takich, że $0 \leqslant k \leqslant n$:

$$\sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix} = n!$$

Wartości $\begin{bmatrix} n \\ k \end{bmatrix}$ dla małych wartości k:

- $k = 0$.
  Podobnie jak w przypadku liczb Stirlinga drugiego rodzaju mamy $\begin{bmatrix} 0 \\ 0 \end{bmatrix} = 1$ oraz $\begin{bmatrix} n \\ 0 \end{bmatrix} = 0$ dla $n > 0$.
- $k = 1$.
  Oczywiście $\begin{bmatrix} 0 \\ 1 \end{bmatrix} = 0$. Pamiętamy, że zbiór n-elementowy ma dokładnie $n!$ permutacji. Każdemu cyklowi odpowiada dokładnie n permutacji (każda rozpoczyna się od innego elementu danego zbioru), zatem

$$\begin{bmatrix} n \\ 1 \end{bmatrix} = \frac{n!}{n} = (n-1)!$$

Twierdzenie

Dla każdej liczby pierwszej p i dla każdej liczby całkowitej dodatniej n zachodzi

$$\alpha_p(n!) < \frac{n}{p-1}$$

Dowód.

$$\alpha_p(n!) < \frac{n}{p} + \frac{n}{p^2} + \frac{n}{p^3} + \ldots = \frac{n}{p}\left(1 + \frac{1}{p} + \frac{1}{p^2} + \ldots\right) = \frac{n}{p} \cdot \frac{p}{p-1} = \frac{n}{p-1}$$

□

Przykład

Wyznaczyć liczby $\varphi(180)$ i $\varphi(12\,936)$.

- Postać kanoniczna liczby 180 to $2^2 \cdot 3^2 \cdot 5$, więc jedynymi dzielnikami pierwszymi danej liczby są 2, 3 i 5. Zatem

$$\varphi(180) = 180 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 48.$$

- $12\,936 = 2^3 \cdot 3 \cdot 7^2 \cdot 11$, więc dzielnikami pierwszymi danej liczby są 2, 3, 7 i 11. Zatem

$$\varphi(12\,936) = 12\,936 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{6}{7} \cdot \frac{10}{11} = 3360.$$

Stwierdzenie

Dla dowolnej liczby pierwszej p i liczby całkowitej dodatniej α zachodzi:

- $\varphi(p) = p - 1$,
- $\varphi(p^\alpha) = p^\alpha \cdot \left(1 - \frac{1}{p}\right)$.

Dowód.

- Liczba pierwsza p jest względnie pierwsza z każdą z liczb $1, 2, \ldots, p - 1$.
- Zauważmy, że jedynie wielokrotności liczby pierwszej p mają wspólny nietrywialny dzielnik z p^α. Zatem w zbiorze $\{1, 2, \ldots, p^\alpha - 1\}$ liczbami niebędącymi liczbami względnie pierwszymi z p^α są

$$1 \cdot p,\ 2 \cdot p,\ \ldots,\ (p^{\alpha-1} - 1) \cdot p,$$

więc ich liczba wynosi $p^{\alpha-1} - 1$. Zatem

$$\varphi(p^\alpha) = (p^\alpha - 1) - \left(p^{\alpha-1} - 1\right) = p^\alpha - p^{\alpha-1} = p^\alpha \left(1 - \frac{1}{p}\right).$$

$\square$

Twierdzenie (NWD jako kombinacja liniowa)

Dla $a, b \in \mathbb{Z}$ takich, że co najmniej jedna z nich jest różna od 0, istnieją $u, v \in \mathbb{Z}$ takie, że

$$\mathrm{NWD}(a, b) = u \cdot a + v \cdot b.$$

Ponadto $\mathrm{NWD}(a, b)$ jest najmniejszą możliwą <u>dodatnią</u> kombinacją liniową a i b.

Przykład

Wyznaczyć najmniejszą dodatnią kombinację liniową liczb 3 i 7 oraz podać jej przykładowe współczynniki.

$$\begin{aligned} \mathrm{NWD}(3, 7) = {} & 1 = 5 \cdot 3 - 2 \cdot 7 \\ & 1 = (-2) \cdot 3 + 1 \cdot 7 \\ & 1 = (-23) \cdot 3 + 10 \cdot 7 \end{aligned}$$

Przykład

Wyznaczyć największy wspólny dzielnik oraz najmniejszą wspólną wielokrotność liczb 48 i 180.
Stosując algorytm Euklidesa otrzymujemy

$$\begin{aligned} 180 &= 3 \cdot 48 + 36 \\ 48 &= 1 \cdot 36 + 12 \\ 36 &= 3 \cdot 12 \end{aligned}$$

Zatem $\mathsf{NWD}(48, 180) = 12$.

Z faktu $\mathsf{NWD}(a, b) \cdot \mathsf{NWW}(a, b) = |a \cdot b|$ otrzymujemy $\mathsf{NWW}(a, b) = \dfrac{|a \cdot b|}{\mathsf{NWD}(a, b)}$.
Zatem

$$NWW(48, 180) = \frac{48 \cdot 180}{12} = \frac{4 \cdot 180}{1} = 720.$$

Wyznaczenie NWW i NWD

Twierdzenie

Niech

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k} \quad \text{oraz} \quad b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_k^{\beta_k}.$$

Wtedy

$$NWD(a,b) = p_1^{\min\{\alpha_1,\beta_1\}} \cdot p_2^{\min\{\alpha_2,\beta_2\}} \cdot \ldots \cdot p_k^{\min\{\alpha_k,\beta_k\}}$$

oraz

$$NWW(a,b) = p_1^{\max\{\alpha_1,\beta_1\}} \cdot p_2^{\max\{\alpha_2,\beta_2\}} \cdot \ldots \cdot p_k^{\max\{\alpha_k,\beta_k\}}.$$

Liczby o jeden większe od iloczynu początkowych liczb pierwszych to tzw. *liczby Euklidesa*:

$$3,\ 7,\ 31,\ 211,\ 2311,\ 30\,031,\ 510\,511, \ldots$$

Definicja

Liczbę

$$E_n = 1 + \prod_{i=1}^{n} p_i$$

nazywamy n*-tą liczbą Euklidesa*.

Do dzisiaj nie wiadomo czy

- jest nieskończenie wiele liczb pierwszych Euklidesa?
- każda liczba Euklidesa jest bezkwadratowa?

Algorytm Euklidesa dla NWD

Niech $a, b \in \mathbb{N}$ i $a > b$.
Po podzieleniu z resztą a przez b otrzymujemy $a = q_1 b + r_1$.
Jeżeli $r_1 = 0$, to NWD$(a, b) = b$.
Jeżeli $r_1 \neq 0$, to dzielimy z resztą b przez r_1 i otrzymujemy $b = q_2 r_1 + r_2$.
Procedura kończy się, gdy dla pewnego indeksu n mamy $r_n \neq 0$ oraz $r_{n+1} = 0$.
Wtedy $NWD(a, b) = r_n$.

$$
\begin{array}{rll}
a &= q_1 \cdot b + r_1 & \qquad 0 < r_1 < b \\
b &= q_2 \cdot r_1 + r_2 & \qquad 0 < r_2 < r_1 \\
r_1 &= q_3 \cdot r_2 + r_3 & \qquad 0 < r_3 < r_2 \\
&\vdots & \qquad \vdots \\
r_{n-2} &= q_n \cdot r_{n-1} + r_n & \qquad 0 < r_n < r_{n-1} \\
r_{n-1} &= q_{n+1} \cdot r_n + 0 &
\end{array}
$$

$$\text{NWD}(a, b) = r_n$$

Poprawność algorytmu Euklidesa

- Algorytm produkuje malejący ciąg liczb całkowitych nieujemnych $r_1 > r_2 > \ldots > r_n$ (jedna liczba w jednym kroku). Zatem algorytm zatrzymuje się po skończonej liczbie kroków (nie większej niż wartość r_1).
- Z własności $\mathrm{NWD}(a, b) = \mathrm{NWD}(a - qb, b)$ otrzymujemy

$$\begin{aligned}\mathrm{NWD}(a, b) = \mathrm{NWD}(b, r_1) = \mathrm{NWD}(r_1, r_2) = \ldots = \mathrm{NWD}(r_{n-1}, r_n) = \\ = \mathrm{NWD}(r_n, 0) = r_n\end{aligned}$$

Twierdzenie

Liczb pierwszych jest nieskończenie wiele.

Dowód.

Załóżmy nie wprost, że teza twierdzenia jest fałszywa, tj. zbiór liczb pierwszych jest skończony. Zatem dla pewnej liczby naturalnej n mamy

$$\mathbb{P} = \{p_1, p_2, \ldots, p_n\}.$$

Niech P będzie następnikiem iloczynu wszystkich elementów powyższego zbioru $\mathbb{P}$:

$$P = 1 + \prod_{i=1}^{n} p_i.$$

Zauważmy, że liczba P przy dzieleniu przez p_i (dla $i = 1, 2, \ldots, n$) daje resztę 1, zatem liczba P nie jest podzielna przez żadną liczbę pierwszą — uzyskaliśmy sprzeczność. $\square$

Powyższy dowód ma ∼2500 lat (*Elementy* Euklidesa).